jamk.fi

Perusturvan tietoturvasuunnitelman laatiminen

Milla Kinnunen

Opinnäytetyö
Maaliskuu 2016
Sosiaali- ja terveysala
Sairaanhoitaja (AMK), hoitotyön tutkinto-ohjelma

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Kinnunen, Milla	Opinnäytetyö, AMK	Maaliskuu 2016
	Sivumäärä 39	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty:

Työn nimi
Perusturvan tietoturvasuunnitelman laatiminen

Tutkinto-ohjelma
Sairaanhoitaja (AMK), hoitotyö

Työn ohjaaja(t)
Pirjo Tiikkainen

Toimeksiantaja(t)
Kinnulan kunta, perusturvatoimiala

Tiivistelmä

Tietotekniikkaa käytetään hoitotyössä yhä enemmän ja hoitohenkilöstön osaamisvaatimukset kasvavat. Opinnäytetyön tarkoituksena on kartoittaa perusturvatoimialan tietoturvariskit ja laatia tietoturvasuunnitelma.

Aineisto kerättiin haastattelemalla Kinnulan kunnan perusturvatoimialan avainhenkilöitä: ylilääkäriä, johtavaa hoitajaa, sosiaalijohtajaa, tietosuojavastaavaa, kunnanrakennusmestaria ja ATK-palveluntuottajaa. Haastatteluilla kartoitettiin tietoturvariskejä osa-alueittain tietoturvasuunnitelman sisällön mukaisesti sekä selvitettiin perusturvatoimialan tietoturvakäytännöt.

Riskikartoituksessa havaittiin välitöntä korjaamista vaativia riskejä ainoastaan yksi, fyysisen turvallisuuden osa-alueella. Kohtalaisia riskejä havaittiin yhteensä neljä, joista kaksi olivat hallinnollisen tietoturvallisuuden osa-alueella. Vähäisiä riskejä oli eniten, yhteensä yhdeksän. Laitteistoturvallisuuden osa-alueella vähäisiä riskejä havaittiin viisi, fyysisen turvallisuuden osa-alueella yksi ja henkilöstöturvallisuuden osa-alueella kolme. Yhteenvetona riskikartoituksesta ilmeni, että yleisellä tasolla henkilöstöresurssien vähyys ja henkilöstön kuormittuminen oli riskitekijä kaikilla osa-alueilla.

Haastatteluiden perusteella saatu tietoaineisto perusturvatoimialan tietoturvakäytännöistä koottiin tietoturvasuunnitelmaksi.

Työssä pohdittiin tietoturvallisuutta hoitotyön näkökulmasta ja verrattiin haastattelussa saatua aineistoa aiempiin tutkimuksiin hoitohenkilöstön tietoturvaosaamisesta. Tulokset olivat samansuuntaiset aiempiin tutkimuksiin verrattuna: hoitohenkilöstöä tulee kouluttaa enemmän tietoturvaan liittyvissä asioissa. Henkilöstön korkeahko keski-ikä huomioiden ei voida olettaa tietoteknisen osaamisen olevan riittävää ilman lisäkoulutusta.

Avainsanat (asiasanat)

Tietoturvallisuus, hoitohenkilöstö, riskikartoitus, tietoturvasuunnitelma

Muut tiedot

jamk.fi

Description

Author(s)	Type of publication	Date
Kinnunen, Milla	Bachelor's thesis	March 2016
		Language of publication: Finnish
	Number of pages 39	Permission for web publication:

Title of publication

Information security plan for the Department of Health and Social Services

Degree programme

Degree Programme in Nursing

Supervisor(s)

Tiikkainen, Pirjo

Assigned by

Kinnula Municipality, Department of Health and Social Services

Abstract

The need of information technology competence is growing among nurses as well as the use of information technology in health care. The goal of the study was to discover the information security risks and to create a data security plan for the Department of Health and Social Services of the Kinnula municipality.

The study was implemented by interviewing the municipality's medical director, the director of nursing services, the director of social services, the data security officer, the director of technical services and the information technology service provider. The interviews provided information about the security risks and the data security practices in the Department of Health and Social services of Kinnula municipality.

Only one significant security risk was discovered in the physical security section. Four medium risks were discovered in total, two of them in the administrative data security section. In total, nine low risks were discovered of which five were in the hardware security section, one in the physical security section and three in the personnel security section. In summary, the shortage of personnel and stress created risks in every section of the data security plan.

The information collected from the interviews was analysed and compiled as the data security plan.

Data security was analysed from the point of view of nursing. The information from the interviews was compared to previous research on the information technology competence of nurses. Parallel results were found: nurses need more data security education. Considering the high average age of the personnel, it is only fair to assume that without further training they would have inadequate IT-skills.

Keywords/tags (subjects)

Information security, nursing, risk management, information security plan

Miscellaneous

Sisältö

Kuviot

Taulukot

1 Johdanto

Tietotekniikkaa käytetään hoitotyössä yhä enemmän. Sähköisiä potilastietojärjestelmiä käytetään maanlaajuisesti (Hämäläinen, Reponen ja Winblad 2012, 4). Uusia tietoteknisiä ratkaisuja hoitotyöhön kehitetään jatkuvasti. Tietotekniikan käytön yleistyessä myös tietoturvallisuuden merkitys kasvaa. On osattava tunnistaa mahdollisia tietoturvariskejä ja sitä kautta pyrittävä ennaltaehkäisemään tietoturvaa vaarantavia tilanteita.

Tietotekniikan käytön lisääntymisen myötä sairaanhoitajien osaamisvaatimukset kasvavat. Sairaanhoitajan osaamisvaatimuksiin kuuluvat mm. keskeiset tieto- ja viestintätekniikan perustaidot sekä tietosuojan ja –turvan mukainen toiminta ja tietous (Opetusministeriö 2006, 63). Jatkuva tietojen päivittäminen on tarpeen, sillä tekniikka kehittyy nopeasti.

TIGER (Technology Informatics Guiding Educational Reform) on kansainvälinen ohjelma, jonka tarkoitus on edistää teknologian sulauttamista hoitotyön käytäntöön ja koulutukseen ja sitä kautta parantaa potilasturvallisuutta ja hoidon laatua (Dulong, 2008). TIGER –ohjelmaan kuuluvan TICC:n (Tiger Informatics Competecies Collaborative) raportissa suositellaan, että kaikkien hoitajien tulisi hallita tietotekniikan perustaidot, informaationlukutaidot ja tiedonhallintataidot. (Ball ym. 2011, 141.)

Tietotekniikan perustaidoista TICC:n suosituksen (2009, 3-7) mukaan kaikkien hoitajien tulisi hallita informaatioteknologin peruskäsitteet, tietokoneen käyttö ja tiedostojen hallinta, tekstinkäsittely sekä Internetin käyttö ja viestintä Internetissä. Informaationlukutaidoissa hoitajan vähimmäisosaamisen tavoitteena on, että hoitajalla on kyky määritellä tarvittava tieto, kyky käyttää ja hankkia tietoa tehokkaasti sekä arvioida tiedon luotettavuutta sekä sen vaikutuksia. Riittävät tiedonhallintataidot takaavat sen, että hoitaja kykenee käyttämään potilastietojärjestelmiä tehokkaasti ja turvallisesti.

2 Tietoturvallisuus terveydenhuollossa

Tietoturvallisuus tarkoittaa niitä järjestelyitä, jolla pyritään varmistamaan tiedon käytettävyys, eheys ja luottamuksellisuus. Tietoturvallisuus terveydenhuollossa käsittää kaikki ne toimenpiteet, joilla estetään potilasta koskevien tietojen joutuminen ulkopuolisten tahojen tietoon tai hallintaan tai tietojen häviäminen tai hävittäminen. (Laine 2004; Valtionhallinnon tietoturvasanasto 2008, 111.)

Tiedon eheydellä tarkoitetaan tietojen tai tietojärjestelmän ristiriidattomuutta, kattavuutta, ajantasaisuutta, oikeellisuutta ja käyttökelpoisuutta. Se on ominaisuus, joka ilmentää, ettei tietoa tai viestiä ole muutettu valtuudettomasti ja että mahdolliset muutokset voidaan todentaa kirjausketjusta. *Tiedon käytettävyys* taas tarkoittaa sitä, että tieto, tietojärjestelmä tai palvelu on siihen oikeutetuille saatavilla ja hyödynnettävissä haluttuna aikana ja vaaditulla tavalla. *Tiedon luottamuksellisuus* tarkoittaa tietojen säilymistä luottamuksellisina ja tietoihin, tietojenkäsittelyyn ja tietoliikenteeseen kohdistuvien oikeuksien säilymistä vaarantumiselta ja loukkauksilta. (Valtionhallinnon tietoturvasanasto 2008, 27; 54; 63.)

Tietoturvan hoidon vaatimukset ja haasteet ovat viimeaikoina kasvaneet, kun asiakas- ja potilastietojen säilytys, käsittely ja siirtäminen sähköisessä muodossa ovat arkipäivää. Tietoriskien hallinta tulee olemaan tulevaisuudessa yhä merkittävämmässä roolissa. (Tammisalo 2007, 9.)

Tietoturvasuunnitelmalla tarkoitetaan riskianalyysiin perustuvaa tietoturvallisuuden arvioinnin tulosta (Valtionhallinnon tietoturvasanasto 2008, 111). *Tietoriski* on tietoon kohdistuva tai tiedosta aiheutuva riski (Valtionhallinnon tietoturvasanasto 2008, 106). *Tietoturvajärjestelyillä* varmistetaan tietoaineistojen, tietojärjestelmien ja palveluiden asianmukainen suojaus siten, että niiden luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvät riskit otetaan huomioon. (Henkilöstön tietoturvaohje 2013.)

2.1 Tietotekniikan käyttö terveydenhuollossa

Hämäläisen, Reposen ja Winbladin (2012, 4-5) mukaan Suomessa vuonna 2011 sähköiset potilaskertomukset olivat käytössä kaikissa julkisen erikoissairaanhoidon ja perusterveydenhuollon toimipisteissä. Sähköisiä lähetteitä käytettiin tutkimuksen mukaan lähes kaikissa sairaanhoitopiireissä ja terveyskeskuksissa. Jokin aluetietojärjestelmä oli käytössä 18:ssa sairaanhoitopiirissä vuonna 2011. Myös laboratoriotulosten sähköistä siirtämistä oli vuonna 2011 käytössä kaikissa sairaanhoitopiireissä ja useimmissa terveyskeskuksissa.

Kansalaisille tarkoitettuja palveluita, kuten suoraa sähköistä ajanvarausta, sähköposti- ja tekstiviestikommunikointia sekä tiedonvaihtoa nettilomakkein oli käytössä vuonna 2011 vain muutamassa terveydenhuollon yksikössä (Mts. 5).

Kaikki julkisen terveydenhuollon yksiköt tallensivat potilaskertomustietoa Potilastiedon arkistoon joulukuussa 2015. Yksityisen terveydenhuollon ensimmäiset potilastiedon arkiston käyttöönotot tapahtuvat alkuvuonna 2016. Joulukuussa 2015 Potilastiedon arkistoon oli arkistoitu yhteensä 301 198 512 asiakirjaa 4 725 516 henkilöstä. (Jormanainen 2016.)

2.2 Tietoturvasuunnitelma

Tietoturvasuunnitelma jaetaan tyypillisesti kahdeksaan osa-alueeseen, joita ovat hallinnollinen turvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus, tietoliikenneturvallisuus, laitteistoturvallisuus, käyttöturvallisuus, ohjelmistoturvallisuus ja tietoaineistoturvallisuus (Paavilainen 1998, 108).

Kuvio 1. Tietoturvasuunnitelman osa-alueet (Paavilainen 1998, 108).

2.2.1 Hallinnollinen tietoturvallisuus

Hallinnollinen tietoturvallisuus tarkoittaa organisaation toimintatapaa, jolla pyritään välttämään ja estämään tietoturvaan liittyviä riskejä. Tietoriskillä tarkoitetaan tilannetta, jolloin tiedon saaminen on estynyt, tieto on muuttunut tapahtuman seurauksena tai joutunut ulkopuolisen haltuun. Riskikartoituksella voidaan paikallistaa uhkia ja analyysin perusteella luoda tarvittava ohjeistus sekä toimintaohjeet. Riskien arvioinnissa tulee käyttää ennalta määrättyjä kriteerejä. Riskin suuruutta arvioidaan mahdollisten seurausten vakavuuden ja todennäköisyyden kautta. (Paavilainen 1998, 48-49; Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa 2003, 5, 41.)

Riskienhallinta ja riskeistä raportointi ovat vaaratilanteiden ennaltaehkäisyn avainasemassa hoitotyössä. Yksi paljon käytetty raportointityökalu on HaiPro-järjestelmä, joka on tarkoitettu yksiköiden sisäisen toiminnan kehittämiseen. (HaiPro 2013.)

2.2.2 Henkilöstöturvallisuus

Henkilöstöturvallisuudella tarkoitetaan henkilöstöstä aiheutuvien tietoturvariskien hallintaa. Henkilöstö on tietoturvan näkökulmasta suurin yksittäinen riskitekijä, koska inhimillisestä toiminnasta voi aina koitua tietoturvavahinkoja. Riskejä voi muodostua salassapitoasioissa ja käytettäessä salassa pidettäviä tietoja ja tietojärjestelmiä. Turvallisuutta lisätään koulutuksilla ja ohjeistuksilla sekä valvomalla henkilöstöä ja vierailijoita. (Paavilainen 1998, 87-89; Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta 2008, 11-12.)

Hoitoala on naisvaltainen ala. Kolme neljäsosaa kunnallisesta henkilöstöstä työskentelee terveydenhuollossa, sosiaalitoimessa tai sivistystoimessa. Neljä viidesosaa henkilöstöstä on naisia. Lakisääteiset perhevapaat oikeuttavat pitkiin poissaoloihin, jolloin sijaisten tarve kasvaa. Henkilöstön suuri vaihtuvuus muodostaa myös riskejä. Henkilöä palkatessa on hänen luotettavuutensa aina tarkistettava. Työsuhteen päättyessä on huolehdittava, ettei kulkulupia, käyttäjätunnuksia ym. jää voimaan. Suuri vaihtuvuus aiheuttaa haasteensa myös henkilöstön tietoturvatietoisuuden näkökulmasta. (Joka viides suomalainen työskentelee kunta-alalla 2015; Paavilainen 1998, 92-93.)

2.2.3 Fyysinen turvallisuus

Fyysisellä turvallisuudella tarkoitetaan laitteisto-, käyttö-, varasto- ja arkistotilojen fyysistä suojaamista. Se on puhtaasti rakennuksiin ja ympäristöön liittyvää. Fyysiseen turvallisuuteen liittyvät kulunvalvonta, tekninen valvonta, vartiointi sekä palo-, vesi-, sähkö-, ilmastointi-, murto- yms. vahinkojen torjunta ja estäminen. Fyysisistä uhkatekijöistä keskeisimmät ovat palo- ja vesivahingot, lämpövauriot, valvomaton liikkuminen sekä laitteiden, ohjelmien tai tietojen varkaudet. (Paavilainen 1998, 95-96.)

Hoitotyön fyysiset tilat on suunniteltava siten, että esimerkiksi hoitajien tietokoneille tai paperisiin asiakirjoihin ole potilailla tai vierailijoilla vapaata pääsyä. Käytännössä tämä tarkoittaa kulunvalvontaa. Pääsy kohteeseen rajoitetaan tunnistuksella, joka perustuu yleensä käyttäjän hallussa, tiedossa tai omistuksessa olevaan asiaan. Näitä voivat olla esimerkiksi muistettavat tunnisteet (salasanat, numerokoodit), tunnistusmateriaali (avaimet, kulkukortit) tai käyttäjän ominaisuudet (puheentunnistus, sormenjäljet). (Paavilainen 1998, 98-99.)

2.2.4 Laitteistoturvallisuus

Laitteistoturvallisuudella tarkoitetaan laitteiden kokoonpanoon, kunnossapitoon ja laadunvarmistukseen liittyvää tietoturvallisuutta. Myös laitteisiin (palvelimiin, tietokoneisiin tulostimiin ja verkkokomponentteihin) suoranaisesti liittyvät varusohjelmat sekä laitteiston elinkaaren turvaamiseen liittyvät asiat, kuten asennus, takuu, ylläpito ja käytöstä poisto, liittyvät laitteistoturvallisuuteen. (Paavilainen 1998, 164-165; Laitteistoturvallisuus 2009.)

2.2.5 Ohjelmistoturvallisuus

Ohjelmistoturvallisuudella tarkoitetaan kaikkien käytettävien ohjelmistojen ja sovellusten tietoturvallisuusominaisuuksia. Ohjelmistoturvallisuuteen kuuluvat ohjelmistoihin liittyvät seikat, kuten ohjelmistoversioiden ja lisenssien hallinta sekä ohjelmistojen testaus, jolla varmistetaan mm. sovellusten sopivuus suunniteltuun käyttötarkoitukseen, ohjelmistojen keskinäinen yhteensopivuus sekä toiminnan luotettavuus ja virheettömyys. Paavilainen 1998, 185; Hakala ym. 2006, 11-12.)

Ohjelmistoturvallisuuden tärkeimpiä perussuojausmenetelmiä ovat ohjelmiston pääsynvalvonta, ohjelmiston tapahtumatietojen seuranta, varmuuskopiointi, asianmukainen ohjelmistodokumentaatio, asianmukaisesti laaditut ylläpito- ja huoltosopimukset sekä rekisteröityjen ohjelmistojen käyttö (Miettinen 1999, 226).

2.2.6 Tietoliikenneturvallisuus

Tietoliikenneturvallisuus koostuu toimenpiteistä, joilla varmistetaan verkoissa välitettävien tietojen luottamuksellisuus, eheys ja käytettävyys. Päämääränä on varmistaa viestien alkuperäisyys, koskemattomuus ja luottamuksellisuus, todentaa lähettäjä ja vastaanottaja, varmentaa tietoliikennelaitteiden fyysinen turvallisuus sekä estää väärinreititys. Tietoliikenneturvallisuuteen kuuluvat kaikki asiat, jotka koskevat verkkojen rakentamista, suunnittelua ja verkkoliikennettä. Tietoliikenneverkkojen uhkia voivat olla esimerkiksi oma henkilöstö, vierailijat, laiteviat, tuhotyöt ja tulipalot, hakkerointi, vakoilu, salakuuntelu, laitteiden häirintä tai manipulointi tai verkon kuormittaminen. (Paavilainen 1998, 108; 137-139.)

Tietoverkko pitää dokumentoida asianmukaisesti ja dokumentointia tulee myös ylläpitää ja valvoa. Tietoliikenneyhteyksistä tulee dokumentoida myös käyttö; dokumenteista tulee ilmetä tietovirrat, tietojen omistajuus sekä tietojen käyttäjät. (Tietoliikenneturvallisuus 2009.)

2.2.7 Tietoaineistoturvallisuus

Tietoaineistoturvallisuus on asiakirjojen, tietueiden, tiedostojen ja muiden tietovälineiden tunnistamista ja turvaluokitusta sekä tietovälineiden hallintaa, säilytystä ja käsittelyä asianmukaisesti kaikissa tiedonkäsittelyprosessien eri vaiheissa. Tietoaineistoturvallisuuteen liittyy olennaisena osana myös tiedon varmistaminen, asianmukainen säilytys ja hävittäminen. (Paavilainen 1998, 26.)

Tietoaineistoon pääsy sallitaan käyttäjän tunnistamisen jälkeen. Tyypillisimpiä tapoja tunnistamiseen ovat henkilökohtainen tuttavuus, avaimet, käyttäjätunnukset ja salasanat sekä toimikortit. (Mts, 26.)

Tietoaineisto on hoitotyössä pääsääntöisesti aina salassa pidettävää. Terveydenhuollon ammattihenkilöiden salassapitovelvollisuudesta on säädetty laissa terveydenhuollon ammattihenkilöistä (559/1994). Terveydenhuollon ammattihenkilö ei saa luovuttaa asemansa tai tehtävänsä perusteella saamaansa tietoa ulkopuoliselle. Salassapitovelvollisuus säilyy myös ammatinharjoittamisen päättymisen jälkeen.

Tietoaineisto voidaan säilyttää ja arkistoida joko sähköisessä tai manuaalisessa muodossa. Tietoaineiston säilytystilojen turvallisuus tulee mitoittaa säilytettävän aineiston kriittisyyden mukaan. Huomioitavia asioita ovat riittävä murtosuojaus, paloturvallisuus, lämpötila, ilman kosteus, pöly, valo jne. Eri tietovälineillä on säilytyksen osalta erityisvaatimuksia. (Tietoaineistoturvallisuus 2009.)

Terveydenhuollon yksiköt voivat tallentaa potilastietoja omista tietojärjestelmistään tietoturvallisesti potilastiedon arkistoon. Potilastiedon arkiston kautta potilastiedot ovat käytettävissä niissä terveydenhuollon toimintayksiköissä, jotka tarvitsevat niitä potilaan hoidossa. Potilastiedon arkistoon tallennetut potilastiedot ovat tiedon tallentaneen terveydenhuollon palvelujen antajan käytettävissä. Tietojen luovuttaminen muille terveydenhuollon palvelujen antajille edellyttää potilaan antamaa suostumusta. Potilas voi kuitenkin rajata suostumuksen laajuutta erikseen tekemällään kiellolla. Suostumuksen tai kiellon tai niiden peruutuksen voi tehdä palveluun liittyneen terveydenhuollon palvelujen antajan luona tai Omakanta-internetpalvelussa. (Potilastiedon arkisto 2015.)

Potilas voi itse seurata potilastiedon arkistosta tehtyjä potilastietojensa luovutuksia Omakanta-palvelun kautta tai pyytää luovutustiedot Kelasta. Terveydenhuollon toimintayksiköiden on lain mukaan valvottava omassa organisaatiossaan potilastietojen käyttöä. Jotta tietoturva toteutuu, terveydenhuollon toimintayksiköt laativat omavalvontasuunnitelman ja huolehtivat suunnitelman mukaisesti käyttöoikeuksista ja lokiseurannasta. Lokitiedot on mahdollista saada kahden edellisen vuoden ajalta, perustellusta syystä myös pidemmältä ajalta. Lokitietopyyntö tehdään Kelan virallisella lomakkeella ja osoitetaan kirjallisesti allekirjoitettuna Kelalle. Tiedot toimitetaan potilaalle kirjallisesti. (Tietojen käyttö ja valvonta 2015.)

2.2.8 Käyttöturvallisuus

Käyttöturvallisuudella tarkoitetaan niitä tietotekniikan käyttöön, käyttöympäristöön, tietojenkäsittelyyn ja sen jatkuvuuteen sekä tuki-, ylläpito-, kehittämis- ja huoltotoimintoihin liittyviä keinoja, joilla parannetaan tietoturvallisuutta (Käyttöturvallisuus 2009).

Potilasturvallisuus taataan potilastietojärjestelmien tietoturvallisella käytöllä. Turvallinen käyttö edellyttää hoitotyössä luotettavaa tunnistautumista järjestelmään, huolellista tiedonkäsittelyä ja myös riittävää tietoteknistä osaamista.

Käyttäjätunnuksen ja salasanan yhdistelmä on yleisin käyttäjän tunnistusmenetelmä. Käyttäjätunnukset ovat julkisia, joten tietoturvan näkökulmasta salasana nousee tärkeään asemaan. Salasanan olisi hyvä täyttää Paavilaisen (1998, 169) mukaan seuraavat vaatimukset:

- *salasanan yhdistäminen käyttäjään tulisi olla mahdollisimman vaikeaa*
- *salasana tulisi vaihtaa pakotetusti tietyin väliajoin*
- *vanhoja salasanoja ei saa käyttää uudelleen*
- *uuden salasanan johtaminen vanhasta ei saa olla mahdollista*
- *salasanalla on oltava tietty vähimmäispituus*
- *salasana tulee antaa sisäänkirjauduttaessa tietyssä ajassa*
- *kolmen virheellisen sisäänkirjautumisen jälkeen käyttöoikeus lukittuu*
- *salasanan paljastuttua käyttäjän tulee voida vaihtaa se välittömästi*
- *salasanojen on oltava salakirjoitettuja, mikäli niitä siirretään julkisessa verkossa*
- *pitää olla olemassa menettely, jolla käyttäjä saa uuden salasanan unohdetun tilalle*
- *salasanoja ei saa tallentaa työaseman kiintolevylle*
- *käyttäjätunnuksen ja salasanan luovuttaminen vieraalle henkilölle on sanktioitava yrityksen sisäisesti.*

Tietojärjestelmiin tunnistauduttaessa hoitotyössä käytetään käyttäjätunnusten ja salasanojen ohella yleisesti toimikorttia. Terveydenhuollon ammattikortin myöntää Väestörekisterikeskus. Ammattikortti myönnetään terveydenhuollon ammattihenkilöille (esim. lääkäri, sairaanhoitaja, farmaseutti tai lääketieteen opiskelija, joka on suorittanut vähintään neljän vuoden lääketieteelliset opinnot). Lisäksi myönnetään terveydenhuollon muun henkilöstön kortteja muille (terveydenhuollon organisaatiossa tai apteekissa työskentelevä henkilö, jolla ei ole terveydenhuollon ammattioikeuksia, esim. sihteeri tai tekninen apulainen). (Terveydenhuollon ammattikortti 2015.)

3 Tietoturva- ja tietotekniikkaosaaminen hoitotyössä

Hoitohenkilöstön tietotekniikka- ja turvaosaamista Suomessa on tutkittu paljon. Yhden suurimmista yksittäisistä riskeistä muodostaa henkilöstön osaamistaso sekä asenne. Koulutus, osaamisen ylläpito ja henkilöstön motivointi sekä riittävät seurantatoimet ovat organisaation toiminnan turvallisuuden avainasemassa. Henkilöstön kouluttaminen on luultavasti helpoin ja varmin keino nostaa tietoturvan tasoa. (Tammisalo 2007, 11.)

Immonen ym. (2003, 195-197) kartoittivat kyselyssään terveydenhuollon organisaatioissa työskentelevien hoitotyöntekijöiden, hallinnollisen ja teknisen henkilöstön sekä lääkäreiden tietotekniikkaan ja tietoturvaan liittyvän koulutuksen määrää, tietotekniikan valmiuksia sekä asenteita tietosuojaa ja tietoturvaa kohtaan. Tutkimuksen kohdehenkilöt valittiin satunnaisotannalla terveydenhuollon kaikista ammattiryhmistä. Tuloksissa mainitaan, että vastaajien tietotekniset valmiudet vaihtelivat hyvän ja keskinkertaisen välillä. Vain harvalla hoitotyöntekijällä oli erittäin hyvät valmiudet. Kaikki vastaajat pitivät tietosuojaa ja turvaa erittäin tärkeänä, mutta kolmasosa vastanneista ei tiennyt oliko heidän organisaatiossaan tietoturvasuunnitelmaa.

Noora von Fieandt (2005, 39-40) kartoitti Pro Gradu-tutkielmassaan erään Helsingin ja Uudenmaan sairaanhoitopiirin sairaalan potilaan hoitoon osallistuvan henkilöstön tietoteknistä osaamista ja koulutustarvetta. Tutkimuksen tulokset osoittivat, että noin 30 % tutkimuskohteen potilaan hoitoon osallistuvasta henkilöstöstä ei osaa käyttää tietokonetta riittävän hyvin työssään. Tutkimuksen mukaan tietotekninen osaaminen riippuu henkilön koulutustasosta, iästä, sukupuolesta ja omasta kiinnostuksesta tietotekniikan käytön suhteen. Alempi peruskoulutus oli yhteydessä huonompiin tietoteknisiin taitoihin. Myös ikä vaikutti osaamistasoon siten, että vanhemmilla työntekijöillä tietotekninen osaaminen oli heikompaa kuin nuoremmilla. Miehet arvioivat tietoteknisen osaamisensa hiukan paremmiksi kuin naiset. Vapaa-ajallaan tietokonetta vähintään kerran viikossa käyttävien taidot olivat paremmat. Ammattiryhmistä osastonsihteereillä oli parhaat työssä tarvittavat tietotekniset taidot. Tietoteknistä koulutusta oli yksikössä järjestetty ja vastanneista lähes 75 % oli osallistunut koulutukseen. Lisäkoulutustarvetta vastaajilla oli kuitenkin kaikilla tietotekniikan osa-alueilla. Eniten koulutustarvetta oli tietotekniikan perusteissa, sähkö-

postin käytössä, Internetin käytössä ja potilastietojärjestelmissä. Vuodeosaston työntekijöillä oli heikommat taidot kuin muiden osastojen henkilöstöllä.

Pirjo Jokelaisen (2011, 1; 58) tutkimuksessa kartoitettiin Kainuun maakuntayhtymän perusterveydenhuollossa sekä erikoissairaanhoidossa työskentelevien hoitohenkilöstön tietoturva- ja tietosuojatietämystä sekä -osaamista. Tutkimustulosten mukaan hoitohenkilöstön tietosuoja- ja tietoturvatietämys ja osaaminen olivat pääsääntöisesti hyvät. Eniten puutetta tiedoissa esiintyi tietojen luovutuskäytäntöjen periaatteista muun muassa viranomaisille ja omaisille. Tutkimuksessa todetaan, että vaikka henkilöstöllä näyttäisikin olevan hyvät valmiudet tietoturvalliseen tiedon hallintaan, lisäkoulutuksen ja toimintatapojen yhtenäisen ohjeistuksen sekä tiedottamisen tarve on ilmeinen liittyen tutkimuksen kohteena olevassa organisaatiossa paraikaa menossa olevaan potilastietojärjestelmien yhtenäistämishankkeeseen. Tutkimuksessa tuotiin esiin myös tietotekniikan ongelmakohtia: salasanojen ja ohjelmien runsaus, tietojen saannin vaikeus ja tietokoneiden hitaus. Tietosuojaan ja tietoturvaan liittyen tutkimuksessa nostettiin esiin kolme asiaa: tietojen päivittämisen ja koulutuksen lisätarve kaikille ammattiryhmille, tietoturvariskien lisääntynyt mahdollisuus (tietokoneen ruudulta voi nähdä toisen asiakkaan tietoja) sekä henkilöstön käyttäytyminen työasemilla (koneiden lukitseminen unohtuu).

Toni Korhosen (2009, 28-29; 43-44) Pro Gradu –tutkielmassa kartoitettiin Etelä-Karjalan sairaanhoitopiirin hoitohenkilöstön tietoturvaosaamista. Tutkimusaineisto hankittiin strukturoidulla verkkokyselylomakkeella, joka välitettiin 597:lle hoitohenkilökuntaan kuuluvalle työntekijälle. Vastausprosentti oli 33, vastaajia 197 henkilöä. Tutkimukseen osallistuneista henkilöistä 68 prosenttia arvioi omat tietotekniset taitonsa työasioissa hyviksi tai erittäin hyviksi. Vastaajista vain alle puolet oli saanut tietoturvakoulutusta. Vähän yli puolet vastanneista oli tyytyväisiä tietoturvallisuusohjeisiin, mutta alle puolet vastanneista piti niitä selkeitä ja ymmärrettävinä. Korhonen toteaa, että koulutukseen ja ohjeistuksien kehittämiseen tulee kiinnittää huomiota. Suurimmiksi riskeiksi hän nimeää tietomurron tekemisen käyttäjän luovuttaman tunnuksen ja salasanan kautta sekä lukitsematta jäävät työasemat.

Anu Laukkasen (2008, 1; 43; 46-49) Pro Gradu tutkielmassa kartoitettiin hoitohenkilöstön tietoturvatietoisuutta ja tietoturvaosaamista. Tutkimuksen kohderyhmänä oli Kuopion yliopistollisen sairaalan operatiivisella tulosalueella työskentelevä hoitohen-

kilöstö. 68 % kyselyyn vastanneista oli sairaanhoitajia. Tutkimus toteutettiin struktu-roidulla neljästä kysymysosiosta koostuvalla lomakkeella, joka lähetettiin kohderyh-mälle sähköpostitse. Kysymysosiot koostuivat tietoturvallisuutta osaamisen, tietoi-suuden ja lainsäädännön näkökulmasta. Vastausprosentti oli 31. Tutkimuksessa tode-taan, että kyseisen kohderyhmän tietoturvatietoisuus ja –osaaminen oli hyvä. Yleiset tietotekniikkataidot olivat hyvät, mutta lisäkoulutusta tarvittaisiin erilaisten työoh-jelmien hallintaan. 73 prosenttia vastaajista oli saanut mielestään tarpeeksi tietotek-niikkakoulutusta, 26 prosenttia vastaajista ilmoitti koulutuksen määrän olleen liian vähäistä. 7-15 vuotta työelämässä olleista vastaajista lisäkoulutuksen näki tarpeelli-seksi 64 prosenttia vastaajista, alle seitsemän vuotta työskennelleillä vastaava luku oli 22 prosenttia. Ikäluokittain tarkasteltuna iäkkäämmät vastaajat kokivat tarvitse-vansa enemmän tietotekniikkakoulutusta kuin nuoremmat vastaajat. Salasanakäy-tännöt olivat kohderyhmän tiedossa. Lainsäädännön vaatimusten tietämyksessä oli pieniä puutteita, kuitenkin henkilötietojen käsittelyä koskeva lainsäädäntö kohde-ryhmällä oli tiedossa. Tietoturvastrategiaan ja työyksikkökohtaisiin ohjeisiin oli tutus-tunut osa henkilöistä.

4 Opinnäytetyön toteuttaminen

Kehittämistyön tarkoituksena on kartoittaa Kinnulan kunnan perusturvatoimialan tietoturvariskejä sekä laatia perusturvatoimialalle tietoturvasuunnitelma. Tietoturvariskejä kartoitettiin haastattelemalla perusturvatoimialan avainhenkilöitä. Haastattelumenetelmänä käytettiin teemahaastattelua. Kysymykset laadittiin Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän tarkistuslistoja apuna käyttäen (Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa 2003, 55-68). Teemahaastattelun kysymykset on esitetty liitteessä 1. Lisäksi käytettiin täydentäviä kysymyksiä tilanteen mukaan.

Haastateltavilta kysyttiin:

1. Millaisia tietoturvallisuusriskejä kunnan perusturvatoimialalla on?

2. Kuinka tietoturvallisuuteen liittyvät asiat kunnan perusturvatoimialalla on järjestetty?

4.1 Haastateltavien valinta

Aineistoa hankkiessa tutkimuksen tarkoituksen toteutuminen on avainasemassa. Tämän vuoksi tiedonantajiksi tulevat henkilöt voidaan myös valita sillä perusteella, että he ovat mahdollisimman hyviä tutkittavan asian asiantuntijoita. Tällaisesta aineistosta käytetään nimitystä harkinnanvarainen otos tai näyte. Harkinnanvaraisessa poiminnassa voidaan käyttää ns. lumipallomenetelmää, jolloin etsitään yksi asiantunteva tiedonantaja, jota pyydetään nimeämään seuraava ja tätä taas seuraava. Joissakin tapauksissa tarvitaan tutkimusaineistoksi kaikki jollain alueella olevat tapaukset tai koko työpaikan henkilöstö, joskus taas voidaan edetä etsimällä tutkimuskohdetta valaisevaa informaatiota niin kauan, ettei uutta tietoa enää saada esiin. (Krause & Kiikkala 1996, 100.)

Haastateltavien valinta tehtiin yhteistyössä toimeksiantajan kanssa. Haastateltaviksi valittiin aluksi ne henkilöt, jotka olivat perusturvatoimialalla johtavassa asemassa: sosiaalijohtaja, ylilääkäri ja johtava hoitaja. Johtavassa asemassa olevat haastatelta-

vat nimesivät tämän jälkeen lisäksi kolme henkilöä haastateltavaksi: perusturvatoimialan tietosuojavastaavan, kunnanrakennusmestarin sekä IT-palveluntuottajan. Perusteluna näiden kolmen henkilön nimeämiselle oli henkilön asiantuntemus tietoturvallisuuteen liittyvissä näkökulmissa.

4.2 Haastattelun toteuttaminen

Haastattelun etuna on, että siinä voidaan säädellä aineiston keruuta joustavasti tilanteen edellyttämällä tavalla ja vastaajia myötäillen. Haastattelutyypit jaetaan tavallisesti kolmeen tyyppiin: strukturoituun eli lomakehaastatteluun, teemahaastatteluun ja avoimeen eli syvähaastatteluun. Strukturoitu haastattelu tapahtuu lomaketta apuna käyttäen, ja kysymysten esittämisjärjestys on ennalta määrätty. Teemahaastattelu on strukturoidun ja avoimen haastattelun välimuoto, siinä haastattelun teemat ovat tiedossa, mutta kysymysten tarkka muoto ja järjestys puuttuvat. Syvähaastattelu on lähimpänä keskustelua, eikä haastattelussa ole varsinaista kiinteää runkoa. (Hirsjärvi, Remes & Sajavaara 2004, 194; 196-199.)

Teemahaastattelussa eli puolistrukturoidussa haastattelussa edetään tiettyjen keskeisten etukäteen valittujen teemojen ja niihin liittyvien tarkentavien kysymysten varassa. On makukysymys, esitetäänkö kaikille haastateltaville kaikki suunnitellut kysymykset tai esitetäänkö ne tietyssä samassa järjestyksessä samoine sanamuotoineen. Teemahaastattelussa pyritään löytämään merkityksellisiä vastauksia tutkimuksen tarkoituksen ja ongelmanasettelun tai tutkimustehtävän mukaisesti. Valitut teemat perustuvat tutkimuksen viitekehykseen eli tutkittavasta ilmiöstä jo tiedettyyn. (Tuomi & Sarajärvi 2002, 77-78.)

Teemahaastattelu toteutettiin haastateltavien työpaikalla ennalta sovittuna ajankohtana. Haastattelua varten pyydettiin varaamaan riittävästi aikaa ja rauhallinen tila. Haastattelut äänitettiin myöhempää analysointia varten. Haastattelut kestivät 45 minuutista 1,5 tuntiin.

4.3 Aineiston analysointi ja tietoturvasuunnitelman laatiminen

Haastatteluaineiston purkaminen aloitettiin kirjoittamalla auki haastatteluäänitteet. Kirjoitettu aineisto luokiteltiin hallinnollisen tietoturvallisuuden, henkilöstöturvallisuuden, fyysisen turvallisuuden, laitteistoturvallisuuden, tietoliikenneturvallisuuden, ohjelmistoturvallisuuden ja tietoaineistoturvallisuuden osa-alueisiin.

Aineiston luokittelun jälkeen siitä etsittiin mahdollisia riskitekijöitä, jotka taulukoitiin. Taulukoinnin jälkeen riskit arvioitiin. Riskiarviossa käytettiin apuna taulukoita 1-3 (Ohje riskien arvioinnissa valtionhallinnossa 41-43).

Taulukko 1. Uhkan todennäköisyys (Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa 2003, 41).

Korkea	3	Toiminto tai järjestelmä on heikosti valvottua Toimintoon tai järjestelmään pääsy on helppoa Toimintoa tai järjestelmää kohtaan on suurta mielenkiintoa Toiminnon ohjeistusta ei ole Tapahtuma ilmenee kerran kuukaudessa Uhkan toteuttaminen on mahdollista suurelle määrälle käyttäjiä
Keski-määräinen	2	Toiminto on osittain valvottua Toiminnon ohjeistus on puutteellista Tapahtuma ilmenee 1-2 kertaa vuodessa Uhkan toteuttaminen on mahdollista tietyille käyttäjäryhmille
Alhainen	1	Toiminto on hyvin valvottua ja siihen pääsy on hallittua Toiminto on hyvin ohjeistettu Toimintoa kohtaan ei ole mielenkiintoa Tapahtuma ilmenee kerran vuodessa Uhkan toteuttaminen on mahdollista vain yksittäisille työntekijöille
Ei merkitystä	0	Uhka ei voi toteutua missään olosuhteissa

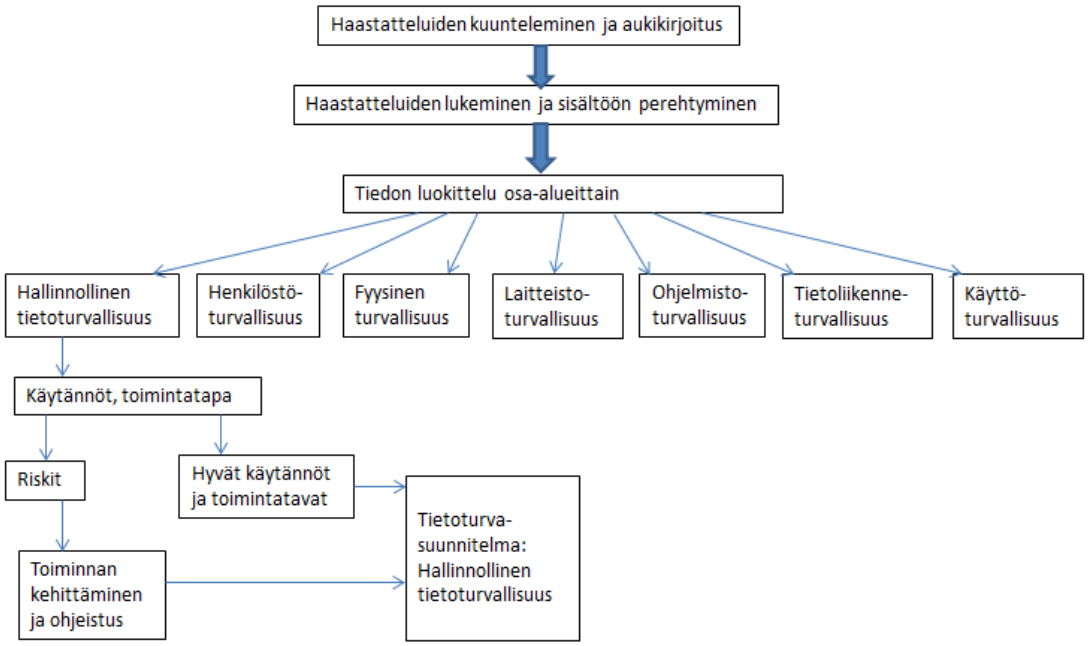
Taulukko 2. Uhkan vakavuus (Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa 2003, 42).

Erittäin vakavat	3	Seuraukset koskevat kaikkia tietojen tai palveluiden käyttäjiä Uhkan toteutuminen aiheuttaa välittömiä toimenpiteitä Uhkan toteutuminen aiheuttaa raportoinnin ministeriölle ja tiedotusvälineille Uhkan toteutuminen aiheuttaa toiminnan keskeytymisen tunneista useisiin päiviin Uhkan toteutuminen aiheuttaa suuria taloudellisia kustannuksia Uhkan toteutuminen aiheuttaa vakavan häiriön organisaation toiminnassa Uhkan toteutuminen aiheuttaa luottamuksellisuuden menetyksen Toiminta on lainsäädännön velvoitteiden vastaista
Vakavat	2	Seurauksilla on vaikutuksia organisaation sisällä Seuraukset koskevat useita tietojen tai palveluiden käyttäjiä Seurauksilla on vaikutus organisaation toimintaan Uhkan toteutuminen aiheuttaa tiedotteen tekemisen Uhkan toteutuminen aiheuttaa merkittäviä taloudellisia kustannuksia
Vähäiset	1	Seuraukset koskevat muutamia tietojen tai palveluiden käyttäjiä Uhkan toteutuminen ei aiheuta välittömästi toimenpiteitä Uhkan toteutuminen aiheuttaa sisäisen raportoinnin Uhkan toteutuminen aiheuttaa vähäisiä taloudellisia kustannuksia Toiminnan keskeytyminen on muutaman minuutin pituinen

Taulukko 3. Riskien arviointi (Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa 2003, 43).

Kriittisyys		Seurausten vakavuus		
		Vähäinen (1)	Vakava (2)	Erittäin vakava (3)
Uhkan todennäköisyys	Korkea (3)	3. Kohtalainen riski	4. Merkittävä riski	5. Sietämätön riski
	Keskimääräinen (2)	2. Vähäinen riski	3. Kohtalainen riski	4. Merkittävä riski
	Alhainen (1)	1. Merkityksetön riski	2. Vähäinen riski	3. Kohtalainen riski

Riskin poistamiseksi tai vähentämiseksi määritettiin toimenpiteitä, joita kirjattiin osaksi tietoturvasuunnitelmaa. Haastatteluaineiston tuloksena saadut hyvät, tietoturvalliset käytänteet ja toimintatavat kirjattiin sellaisenaan tietoturvasuunnitelmaan.



Kuvio 2. Aineiston analysointi ja tietoturvasuunnitelman laatiminen.

Kuviossa 2 on esitetty aineiston analysointi ja tietoturvasuunnitelman laatiminen hallinnollisen tietoturvallisuuden osa-alueen osalta. Tietoturvasuunnitelma koottiin jokaisen osa-alueen kohdalla vastaavalla menetelmällä.

5 Tietoturvasuunnitelma perusturvatoimialalle

Tietoturvasuunnitelma muodostettiin olemassa olevista hyvistä tietoturvakäytännöistä sekä havaittujen riskien perusteella laadituista uusista käytännöistä.

5.1 Hallinnollinen tietoturvallisuus

Teksti poistettu salassapitosyistä

Taulukko 4. Hallinnolliseen tietoturvallisuuteen liittyvät riskit

Riski	**Arviointi**	**Toimenpiteet**
Teksti poistettu salassapitosyistä	Kohtalainen Todennäköisyys 2 Vakavuus 2	Teksti poistettu salassapitosyistä
Teksti poistettu salassapitosyistä	Kohtalainen Todennäköisyys 2 Vakavuus 2	Teksti poistettu salassapitosyistä

Teksti poistettu salassapitosyistä

Tietoturvasuunnitelman hallinnollisen tietoturvallisuuden osa-alueen alle koottiin tehtävät sekä vastuualueet.

Taulukko 5. Tehtävät ja vastuut.

Tehtävä	**Vastuualue**
Sosiaalijohtaja	Teksti poistettu salassapitosyistä
Ylilääkäri	Teksti poistettu salassapitosyistä
Johtava hoitaja	Teksti poistettu salassapitosyistä
Tietosuojavastaava	Teksti poistettu salassapitosyistä
Ohjelmistojen pääkäyttäjät	Teksti poistettu salassapitosyistä
Kunnanrakennusmestari	Teksti poistettu salassapitosyistä
Arkistonhoitaja	Teksti poistettu salassapitosyistä
IT-palveluntuottaja	Teksti poistettu salassapitosyistä
Henkilöstö	Teksti poistettu salassapitosyistä

Teksti poistettu salassapitosyistä

5.2 Henkilöstöturvallisuus

Henkilöstöturvallisuuden alueelle kuuluvat kaikki henkilöstöön liittyvät tietoturva-asiat. Henkilöstöturvallisuuteen liittyviä riskejä havaittiin yhteensä viisi.

Teksti poistettu salassapitosyistä

Taulukko 6. Henkilöstöturvallisuuteen liittyvät riskit

Riski	**Arviointi**	**Toimenpiteet**
Teksti poistettu salassapitosyistä	Kohtalainen Todennäköisyys 1 Vakavuus 3	Teksti poistettu salassapitosyistä
Teksti poistettu salassapitosyistä	Kohtalainen Todennäköisyys 1 Vakavuus 3	Teksti poistettu salassapitosyistä
Teksti poistettu salassapitosyistä	Vähäinen Todennäköisyys 1 Vakavuus 2	Teksti poistettu salassapitosyistä
Teksti poistettu salassapitosyistä	Vähäinen Todennäköisyys 1 Vakavuus 2	Teksti poistettu salassapitosyistä
Teksti poistettu salassapitosyistä	Vähäinen Todennäköisyys 1 Vakavuus 2	Teksti poistettu salassapitosyistä

Teksti poistettu salassapitosyistä

5.3 Fyysinen turvallisuus

Fyysisen turvallisuuden osa-alue käsittelee tietoturvaa rakennusten ja toimitilojen näkökulmasta.

Teksti poistettu salassapitosyistä

Taulukko 7. Fyysiseen turvallisuuteen liittyvät riskit

Riski	**Arviointi**	**Toimenpiteet**
Teksti poistettu salassapitosyistä	Merkittävä Todennäköisyys 3 Vakavuus 2	Teksti poistettu salassapitosyistä
Teksti poistettu salassapitosyistä	Vähäinen Todennäköisyys 2 Vakavuus 1	Teksti poistettu salassapitosyistä

Teksti poistettu salassapitosyistä

5.4 Tietoliikenneturvallisuus ja laitteistoturvallisuus

Teksti poistettu salassapitosyistä

Taulukko 8. Laitteistoturvallisuuteen liittyvät riskit

Riski	**Arviointi**	**Toimenpiteet**
Teksti poistettu salassapitosyistä	Vähäinen Todennäköisyys 1 Vakavuus 2	Teksti poistettu salassapitosyistä
Teksti poistettu salassapitosyistä	Vähäinen Todennäköisyys 1 Vakavuus 2	Teksti poistettu salassapitosyistä
Teksti poistettu salassapitosyistä	Merkityksetön Todennäköisyys 1 Vakavuus 1	Teksti poistettu salassapitosyistä
Teksti poistettu salassapitosyistä	Vähäinen Todennäköisyys 1 Vakavuus 2	Teksti poistettu salassapitosyistä
Teksti poistettu salassapitosyistä	Vähäinen Todennäköisyys 1 Vakavuus 2	Teksti poistettu salassapitosyistä
Teksti poistettu salassapitosyistä	Vähäinen Todennäköisyys 1 Vakavuus 2	Teksti poistettu salassapitosyistä

Teksti poistettu salassapitosyistä

5.5 Tietoaineistoturvallisuus

Teksti poistettu salassapitosyistä

Taulukko 9. Tietoaineistoturvallisuuteen liittyvät riskit

Riski	**Arviointi**	**Toimenpiteet**
Teksti poistettu salassapitosyistä	Kohtalainen Todennäköisyys 1 Vakavuus 3	Teksti poistettu salassapitosyistä

Teksti poistettu salassapitosyistä

5.6 Liittyvät dokumentit ja niiden sijainti

Olemassa olevasta ohjeistuksesta ja dokumenteista tehtiin tietoturvasuunnitelman loppuun luettelo, josta ilmenee dokumenttien sijainti:

Teksti poistettu salassapitosyistä

6 Pohdinta

6.1 Tulosten tarkastelu

Opinnäytetyön tarkoituksena oli laatia kunnan perusturvatoimialan tietoturvasuunnitelma, jota ei tässä laajuudessa ollut toteutettu aiemmin. Myöskään riskianalyysia ei ollut toimialalla tehty. Haastattelujen pohjalta saatiin tietoa tietoturvariskeistä ja laadittiin ehdotettuja kehittämistoimenpiteitä. Tietoturvasuunnitelma on asiakirja, jota tulee päivittää säännöllisesti mahdollisten uusien havaittujen riskien seurauksena.

Kehittämistyön tuloksena havaittiin merkittäviä, välitöntä korjaamista vaativia riskejä ainoastaan yksi fyysisen turvallisuuden osa-alueella. Kohtalaisia riskejä havaittiin yhteensä neljä, joista kaksi olivat hallinnollisen tietoturvallisuuden osa-alueella, yksi henkilöstöturvallisuuden osa-alueella ja yksi tietoaineistoturvallisuuden osa-alueella. Vähäisiä riskejä oli eniten, yhteensä yhdeksän. Laitteistoturvallisuuden osa-alueella vähäisiä riskejä havaittiin viisi, fyysisen turvallisuuden osa-alueella yksi ja henkilöstöturvallisuuden osa-alueella kolme. Myös pienet riskit kirjattiin, merkityksettömiä riskejä löydettiin yksi laitteistoturvallisuuden osa-alueelta.

Tietoturvallisuuteen kuuluu, että vastuualueet on määritetty selkeästi. Koulutuksen määrän tulee olla riittävä ja huolehtia asianmukaisesta perehdytyksestä myös tietoturvallisuutta koskevissa asioissa.

Useat tutkimukset korostavat riittävän koulutuksen ja ohjeistuksen tärkeyttä tietoturvallisuuden toteutumiseksi (Immonen ym. 2003, 195-197; Jokelainen 2011, 1; 58; Korhonen 2009, 28-29; 43-44; Laukkanen 2008, 1; 43; 46-49 ; von Fieandt 2005, 39-40). Haastatteluissa tuli ilmi useassa eri yhteydessä, että tietoturva-asioista ei järjestetä riittävästi koulutusta. Jos koulutuksen määrä on vähäistä, jää hoitohenkilöstön tietoturvaosaaminen väistämättä puutteelliseksi. Ei voida olettaa, että henkilöstöllä olisi entuudestaan riittävä tietämys asian hallitsemiseksi.

Kirjallisten ohjeiden puute sekä resurssipulasta aiheutuva kiire aiheuttivat haastatteluiden mukaan riskejä. Myös henkilöstön suuri vaihtuvuus muodosti riskitekijän, sillä perehdyttämiseen ei käytetty tarpeeksi aikaa. Riittävällä ohjeistuksella ehkäistään myös käyttäjätunnusten ja salasanojen väärinkäyttöä. Tarkempaa ohjeistusta olisi syytä laatia mm. muistitikkujen säilytyksestä ja siitä, millaista tietoa niille voi tallentaa sekä älypuhelimen käytöstä.

Kinnulan kunnan perusturvan henkilöstössä on vain vähän nuoria työntekijöitä. Kinnulan kunnan vakituisen hoitohenkilöstön keski-ikä tammikuussa 2016 oli 48,7 vuotta (Hautsalo 2016). Koulutuksen merkitys korostuu myös tässä suhteessa. Työntekijän iän ja lisäkoulutuksen tarvetta on kartoitettu mm. Noora von Fieandtin (2005, 39-40) tutkimuksessa. Tutkimuksen mukaan hoitohenkilöstön tietotekninen osaaminen riippuu henkilön koulutustasosta, iästä, sukupuolesta ja ennen kaikkea omasta kiinnostuksesta tietotekniikan käytön suhteen. Mitä alempi peruskoulutus vastaajalla oli, sen huonommat olivat hänen taitonsa. Vastaajan ikä vaikutti siten, että vanhemmilla työntekijöillä tietotekninen osaaminen oli heikompaa kuin nuoremmilla.

Nyt, kun tietoturvasuunnitelma on laadittu, on erityisen tärkeää viedä tietoa myös hoitohenkilöstölle. Ei riitä, että suunnitelma on johtavien viranhaltijoiden tiedossa. Tietoturvallisuus ei voi toteutua täydellisesti, jos tietoturvakäytännöistä tiedotetaan puutteellisesti. Esimerkiksi Immosen ym. (2003, 195-197) tutkimuksessa todettiin, että kolmasosa tutkimukseen osallistuneista ei tiennyt oliko heidän organisaatiossaan tietoturvasuunnitelmaa. Jos tietoturvan olemassa olosta ei tiedetä, kuinka sitä voitaisiin toteuttaa?

6.2 Eettisyys ja luotettavuus

Julkishallinnollisen organisaation ollessa tutkimuskohteena henkilöiden nimettömyyden säilyminen ei ole välttämättä mahdollista. Henkilöt osallistuvat tutkimukseen ammatillisen roolinsa yksittäisinä edustajina. Henkilöille ei tällöin voi luvata täyttä tunnistamattomuutta. Tutkimuksen eettisyys korostuu tällöin tutkimusjulkaisun kirjoitustavassa, jossa kunnioitetaan yksittäisiä haastateltavia. (Yksityisyys ja tietosuoja 2013.)

Kehittämistyön eettisyys varmistettiin siten, ettei yksityiskohtaisia tutkimustuloksia luovuteta julkisuuteen. Tietoturvasuunnitelman tiedot pidetään salaisina. Myös äänitetyt haastattelut tuhottiin analysoinnin jälkeen.

Luotettavuuden tarkastelu alkaa tutkimustehtävän tarkastelusta ja siitä, antaako tutkimusaineisto vastauksen tutkimuskysymykseen (Krause & Kiikkala 1996, 130). Aineistonkeruumenetelmänä teemahaastattelu oli onnistunut, sillä esimerkiksi kyselylomake olisi saattanut aiheuttaa sen, että vastaaja olisi ymmärtänyt kysymyksen väärin. Nyt haastatteluissa oli mahdollista tarkentaa, mihin asiaan haastateltavalta haettiin vastausta.

Tutkimuksen luotettavuutta voidaan parantaa selostamalla tarkasti tutkimuksen toteuttaminen. Aineiston tuottamisen olosuhteet kerrotaan selvästi ja totuudenmukaisesti. Haastattelututkimuksessa voidaan kertoa olosuhteista ja paikoista, joissa aineistot kerättiin, samoin kuin haastatteluihin käytetty aika, mahdolliset häiriötekijät, virhetulkinnat haastattelussa sekä tutkijan oma itsearviointi tilanteesta. (Hirsjärvi ym. 2004, 217.)

Haastattelutilanteeseen varattiin runsaasti aikaa ja rauhallinen huone, jossa haastateltava sai rauhassa keskittyä vastaamiseen. Häiriötekijöitä ei ollut, lukuun ottamatta ylilääkärin haastattelua. Hänen kohdallaan haastattelu keskeytettiin hetkeksi kiireellisen konsultoinnin vuoksi. Haastattelua jatkettiin myöhemmin samana päivänä tilanteen rauhoituttua.

Vastaustuloksissa saatiin yksittäisiä vastauksia, jotka poikkesivat muiden haastateltavien vastauksista. Näissä tapauksissa käytettiin täydentäviä kysymyksiä, jotta voitiin varmistua vastauksen oikeellisuudesta. Poikkeamat johtuivat lähinnä siitä, ettei vastaajalla ollut riittävää tietoa erityistä asiantuntijuutta (esimerkiksi yksityiskohtaisia tietoteknisiä seikkoja) vaativissa kysymyksissä.

6.3 Johtopäätökset

Johtopäätöksenä riskienhallinnassa korostuu ennaltaehkäisyn merkitys. Riskienhallintaan pitäisi kiinnittää jatkossa enemmän huomiota. Riskikartoitukset on syytä tehdä säännöllisin väliajoin. Yhteenvetona riskikartoituksesta voidaan sanoa, että yleisellä tasolla henkilöresurssien vähyys, henkilöstön kuormittuminen ja koulutuksen puute oli yleinen riskitekijä kaikilla osa-alueilla. Kehittämistyötä tehdessä ilmeni, että riskienhallintaan pitäisi kiinnittää jatkossa enemmän huomiota. Riskikartoitukset on syytä tehdä säännöllisin väliajoin. Ennaltaehkäisyn merkitystä ei voi koskaan korostaa liikaa tietoturva-asioissa, jotta voidaan säästyä turhilta taloudellisilta kustannuksilta. Jatkossa olisi aiheellista tehdä kaikilla kunnan toimialoilla riskikartoitus ja selvittää tietoturvasuunnitelman ajantasaisuus.

Hoitohenkilöstön tietoturvaosaamisen näkökulmasta esiin nousivat seuraavat asiat:

1. Koulutuksen määrä koettiin liian vähäiseksi. Tietoturvakoulutus pitäisi toteuttaa säännöllisin väliajoin.
2. Uudet työntekijät ja sijaiset pitäisi perehdyttää työsuhteen alussa myös tietoturva-asioihin.
3. Henkilöstöllä ei ole riittävästi aikaa perehtyä ohjeisiin.

TIetoturvasuunnitelma tulee käydä läpi säännöllisin väliajoin ja päivittää sitä tarvittaessa. Jatkotutkimusehdotuksena esitetään, että kunnassa tehtäisiin henkilöstön laajempi tietoturvaosaamiskartoitus.

Lähteet

Ball, M., Douglas, J.V., Hinton Walker, P., DuLong, D. Gugerty, B., Hannah, K.J., Kiel, J., Newbold, S.K., Sensmeier, J.E., Skiba, D.J., ja Trhoseth, M.R. 2011. Nursing Informatics. Where Technology and Caring Meet. Neljäs painos. Lontoo: Springer Science & Business Media.

Dulong, D. 2008. Informatics: The Tiger Project. The Online Journal of Issues in Nursing. Vol. 13 No 2. Internet-sivut. Viitattu 6.2.2016. http://www.nursingworld.org, Member Benefits, ANA Periodicals, OJIN: The Online Journal of Issues in Nursing, Table of Contents, Vol. 13 – 2008, Number 2: May 2008, Columns

HaiPro 2013. Haipro. Terveydenhuollon vaaratapahtumien raportointijärjestelmä. Internet-sivut. Viitattu 14.1.2015. http://www.haipro.fi

Hakala M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Docendo Finland Oy.

Hautsalo, Aulikki 2016. Johtava hoitaja. Kinnulan kunta. Puhelinkeskustelu 3.2.2016.

Henkilöstön tietoturvaohje 2013. Valtiovarainministeriö. Vahti-ohjeet 4/2013. Internet-sivut. Viitattu 8.2.2016. www.vahtiohje.fi

Hämäläinen, P., Reponen, J. ja Winblad, I. 2012. Tieto- ja viestintäteknologian käyttö terveydenhuollossa vuonna 2011 – Tilanne ja kehityksen suunta. Tampere: Juvenes Print Oy – Tampereen yliopistopaino Oy. Viitattu 4.2.2016. http://julkari.fi/bitstream/handle/10024/80372/825d0af8-f97c-4192-bf5b-ba5e1bf773aa.pdf?sequence=1

Immonen, A., Ruotsalainen, P., Saranto, K. ja Turunen, P. 2003. Terveydenhuollon ammattilaisten tietotekniikka- ja tietoturvavalmiudet. Suomen lääkärilehti. Terveydenhuoltoartikkeli. 2/2003 vsk 58. s. 195 – 197

Joka viides suomalainen työskentelee kunta-alalla 2015. Kuntatyönantajat. Internet-sivut. Viitattu 4.2.2016. http://www.kuntatyonantajat.fi/, Kunta työnantajana, Kuntien henkilöstö.

Jokelainen, P. 2011. Hoitohenkilöstön tietosuoja- ja tietoturvatietämys. Pro gradu – tutkielma. Itä-Suomen yliopisto. Yhteiskuntatieteiden ja kauppatieteiden tiedekunta. Sosiaali- ja terveysjohtamisen laitos, sosiaali- ja terveydenhuollon tietohallinto.

Jormanainen, V. 2016. Sote-muutosta mahdollistetaan Kanta-palveluilla. Terveyden ja hyvinvoinnin laitos. Internet-sivut. Viitattu 8.2.2016. http://www.kanta.fi/documents/10180/4105896/Vesa+Jormanainen/6c516097-ca0f-4e81-8c26-ba0b284a4af4

Korhonen, T. 2009. Terveydenhuollon henkilöstön tietoturvaosaaminen. Pro Gradu – tutkielma. Sosiaali- ja terveydenhuollon tietohallinto. Kuopion yliopisto. Terveyshallinnon ja –talouden laitos.

Krause, K. ja Kiikkala, I. 1996. Hoitotieteellisen tutkimuksen peruskysymyksiä. Helsinki:Kirjayhtymä Oy.

Käyttöturvallisuus 2009. Valtiovarainministeriö. Vahti-ohjeet. Internet-sivut. Viitattu 20.3.2014. https://www.vahtiohje.fi/web/guest/kayttoturvallisuus1

Laine, A. 2004. Terveydenhuollon tietoturvallisuus valvovan viranomaisen näkökulmasta. Suomen lääkärilehti. 2004;59(38):3527-3529

Laitteistoturvallisuus 2009. Valtiovarainmisteriö. Vahti-ohjeet. Laitteistoturvallisuus. Internet-sivut. Viitattu 20.3.2014. https://www.vahtiohje.fi/web/guest/laitteistoturvallisuus

L 28.6.1994/559. Laki terveydenhuollon ammattihenkilöstä. Viitattu 4.2.2016. Valtion säädöstietopankki Finlex. http://www.finlex.fi, ajantasainen lainsäädäntö.

Laukkanen, A. 2008. Hoitohenkilöstön tietoturvatietoisuus ja tietoturvaosaaminen. Pro Gradu –tutkielma. Sosiaali- ja terveydenhuollon tietohallinto. Kuopion yliopisto. Terveyshallinnon ja –talouden laitos.

Miettinen, J. 1999. Tietoturvallisuuden johtaminen – näin suojaat yrityksesi toiminnan. Helsinki: Kauppakaari OYJ.

Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa 2003. Valtiovarainministeriö. Vahti 7/2003. Helsinki: Edita Prima Oy.

Opetusministeriö 2006. Opetusministeriön työryhmämuistioita ja selvityksiä 2006:24; Ammattikorkeakoulusta terveydenhuoltoon, Koulutuksesta valmistuvien ammatillinen osaaminen, keskeiset opinnot ja vähimmäisopintopisteet. Opetusministeriön työryhmämuistioita ja selvityksiä 24. Internet-sivut. Viitattu 6.2.2016. http://www.minedu.fi/export/sites/default/OPM/Julkaisut/2006/liitteet/tr24.pdf?lang=fi

Paavilainen, J. 1998. Tietoturva. Jyväskylä: Gummerus Kirjapaino Oy.

Potilastiedon arkisto 2015. Kanta. Internet-sivut. Viitattu 14.1.2016. http://www.kanta.fi, E-arkisto-esittely.

Tammisalo, T. 2007. Sosiaali- ja terveydenhuollon organisaatioiden tietoturvan hallinnointi. Periaatteet ja menetelmät. Stakes, Raportteja 5/2007. http://www.stakes.fi/verkkojulkaisut/raportit/R5-2007-VERKKO.pdf

Terveydenhuollon ammattikortti 2015. Kanta. Internet-sivut. Viitattu 14.1.2016. http://www.kanta.fi, Ammattilaisille, Ammattikortti.

TICC 2009. TIGER Informatics Competecies Collaborative Final Report. Internet-sivut. Viitattu 6.2.2016. http://tigercompetencies.pbworks.com/f/TICC_Final.pdf

Tietoaineistoturvallisuus 2009. Valtiovarainministeriö. Vahti-ohjeet. Internet-sivut. Viitattu 20.3.2014. https://www.vahtiohje.fi/web/guest/tietoaineistoturvallisuus

Tietojen käyttö ja valvonta 2015. Kanta. Internet-sivut. Viitattu 14.1.2016. http://www.kanta.fi, Ammattilaisille, Tietojen käyttö ja valvonta.

Tietoliikenneturvallisuus 2009. Valtiovarainministeriö. Vahti-ohjeet. Internet-sivut. Viitattu 20.3.2014. https://www.vahtiohje.fi/web/guest/tietoliikenneturvallisuus

Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta 2008. Valtiovarainministeriö. Vahti 2/2008. Helsinki: Edita Prima Oy.

Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohje 2000. Vahti 2/2000. Internet-sivut. Viitattu 8.5.2014. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/3386/3388_fi.pdf

Von Fieandt, N. 2005. Henkilöstön tietotekninen osaaminen ja koulutustarve terveydenhuollossa. Pro gradu tutkielma. Sosiaali- ja terveydenhuollon tietohallinto. Kuopion yliopisto. Terveyshallinnon ja talouden laitos.

Valtionhallinnon tietoturvasanasto 2008. Valtiovarainministeriö. Vahti 8/2008. Internet-sivut. www.vahtiohje.fi, Valtionhallinnon tietoturvasanasto.

Yksityisyys ja tietosuoja 2013. Tampereen yliopisto. Internet-sivut. Viitattu 12.2.2016. www.uta.fi, Tutkimus, Tutkimusetiikka, Yksityisyys ja tietosuoja.

Liitteet

Liite 1. Teemahaastattelun kysymykset

Hallinnollinen tietoturvallisuus

- Mitkä ovat esimiehen tehtävät ja vastuut?
- Mitkä ovat tietoturvavastaavan tehtävät ja vastuut?
- Mitkä ovat ATK-tuen tehtävät ja vastuut?
- Mitkä ovat työntekijöiden tehtävät ja vastuut?
- Kuinka tehtävät on vastuutettu?
- Kuinka tietoturvavastuut on määritelty?
- Miten huolehditaan tärkeiden tehtävien varahenkilöjärjestelyistä?
- Kuinka turvallisuuden kehittämistarpeet tunnistetaan?
- Onko turvallisuuden kehittämistarpeet kirjattu kehittämissuunnitelmaksi?
- Onko perusturvatoimialalle tehty selkeä johdon hyväksymä tietoturvallisuuspolitiikka?
- Onko kehittämiskustannuksia arvioitu?
- Miltä osin toiminta vakuutetaan?
- Miten toimitaan, jos epäillään väärinkäytöksiä?

Henkilöstöturvallisuus

- Miten käyttöoikeuksia on rajattu?
- Tiedätkö hyvän salasanan vaatimukset?
- onko henkilöstöä ohjeistettu, ettei saa käyttää esim. samoja salasanoja Facebookissa?
- käytetäänkö koneita henkilökohtaisten asioiden hoitoon (esim. Facebook)?
- kuinka usein henkilöstölle järjestetään koulutuksia tietoturva-asioista?
- onko henkilöstöllä riittävästi aikaa perehtyä ohjeisiin?
- minkälaisia tietoturvariskejä on havaittu inhimillisen virheen seurauksena?
- kuinka riskien raportointi tapahtuu?
- kuinka havaitut virheet käsitellään?
- onko työtehtävien tekemättä jättämisestä koitunut tietoturvariskejä, minkälaisia?
- onko huolimaton tietojenkäsittely aiheuttanut tietoturvariskejä, minkälaisia?
- miten tietojenkalasteluun (phishing) on varauduttu?
- kuinka salassapitovelvollisuutta valvotaan?
- kuinka usein salassapitoa koskevista asioista järjestetään koulutusta?
- onko sisäisten tietojen väärinkäytön mahdollisuutta (harjoittelijat, sähköasentajat, siivoojat…)?
- Kuinka henkilötietojen suojaamisesta on huolehdittu kaikissa niiden käsittelyvaiheissa (sekä sähköisen että manuaalisen aineiston osalta)?
- Kuinka työntekijät on perehdytetty henkilötietojen käsittelyyn ja siihen liittyviin vastuisiin (mm. salassapito- ja vaitiolovelvollisuuteen)?

- Minkälaisia sähköisiä viestittämiskeinoja työssä käytetään (tekstiviestit, sähköpostit…)?
- Kuinka henkilöstöä ohjeistetaan sähköpostin käyttöön liittyvistä asioista (esimerkiksi mitä saa lähettää)?
- Miten henkilön taustat tarkistetaan rekrytointivaiheessa?
- Onko mahdollista, että työsuhteen päättymisen seurauksena voisi hävitä tietoja?

Fyysinen turvallisuus

- Kuinka turvallisuus on otettu huomioon kaapeloinnissa ja johdotuksissa?
- Miten laitteistot, asiakirjat ym. on suojattu varkauden ja ilkivallan varalta?
- Miten laitteistot, asiakirjat ym. on suojattu tulipalon varalta?
- Miten laitteistot, asiakirjat ym. on suojattu vesivahingon varalta?
- Millainen käytäntö on avainten säilytykseen ja käyttämiseen?
- Millaisia hälyttimiä ja valvontalaitteita on käytössä?

Laitteistoturvallisuus

- Kuinka usein laitteistoja huolletaan ja tarkastetaan?
- Kuinka huoltoa valvotaan?
- Millaisia haittoja työskentelyyn laitteen rikkoontumisesta on koitunut?
- Kuinka uuden laitteen käyttöön perehdytetään?
- Minkälaista rekisteriä laitteistosta pidetään?
- Kuinka laitteiden varastaminen on estetty?
- Kuinka muistitikkuja säilytetään ja minkälaista aineistoa niille on sallittua tallentaa?
- Minkälainen ohjeistus on älypuhelinten käytöstä?
- Kuinka älypuhelinten suojaus on toteutettu?
- Kuinka sähkökatkoksilta on suojauduttu?
- Kuinka virtapiikeiltä on suojauduttu?
- Miten jatkuva sähkönsyöttö on turvattu niille laitteille, jotka sitä tarvitsevat?

Tietoliikenneturvallisuus

- Kuinka etäyhteyden kautta tapahtuva työskentely on suojattu?
- kuinka tietoverkko on dokumentoitu?
- Miten tietoverkkoa ylläpidetään ja valvotaan?
- Miten poikkeusoloihin on varauduttu?

Ohjelmistoturvallisuus

- Miten ohjelmistojen ajantasaisuudesta huolehditaan?
- Miten laitteiden välinen tiedonsiirto on suojattu?
- Miten on hoidettu ohjelmistojen lisenssit, päivitykset, säilytys?

- Miten webkamerat ja laitteiden mikrofonit on suojattu?
- Kuinka roskapostin suodatus on hoidettu?
- Voiko käyttäjä asentaa koneelle/puhelimelleen omia ohjelmiaan/tuntemattoman valmistajan sovelluksia?

Tietoaineistoturvallisuus

- Kuinka manuaalista aineistoa säilytetään?
- Kuinka hyvin tiedostetaan, mitkä kaikki tietojoukot ovat henkilörekistereitä (paperikortistot, kehityskeskusteluaineistot, lokitiedostot…)?
- Miten rekisteriselosteet on laadittu ja missä niitä säilytetään?
- Kuinka henkilöstöä koskevan luottamuksellisten ja arkaluontoisten tietojen käsittely on ohjeistettu koko tiedon elinkaaren ajalta ja sen kaikissa olomuodoissa?
- Minkälainen arkistonmuodostussuunnitelma ja arkistotoimen toimintaohje on asiakirjallisen tietoaineiston käsittelyä varten?
- Millaisia ohjeista salaisten asiakirjojen arkistoinnista on annettu?
- Miten arkistotilojen käyttöä valvotaan?
- Miten asiakastiloissa liikkumista valvotaan?
- Millaisia salassapitositoumuksia laaditaan?
- Tiedostaako henkilöstö mitkä ovat arkaluontoisia tietoja ja kuinka niiden käsittely on ohjeistettu?
- Miten tarpeettomien asiakirjojen hävitys tapahtuu?

Seuranta ja päivitys

- Kuinka tietoturvasuunnitelman päivityksestä huolehditaan?
- Kuinka tietoturvan toteutumista seurataan?